IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF UTAH

IN RE SEARCH WARRANT IN THE MATTER OF THE SEARCH OF: SEE ATTACHMENT A	**Case No.** 2:23mj924 CMR

AFFIDAVIT

I, Alaina Dussler, being duly sworn, declare and state as follows:

INTRODUCTION

1. I am a Special Agent ("SA") with the Department of Homeland Security ("DHS"), U.S. Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"). I have held such a position since December 2021. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. I am currently assigned to the Office of the Special Agent in Charge ("SAC"), Seattle, Washington, and am a member of the Child Exploitation Investigations Group. As part of my current duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and

2252A. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)).

2. As part of my current duties as an HSI Criminal Investigator, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code, Sections 2251(a), 2252(a)(2), 2252(a)(4)(B), and 2243(a)(1). I have received training about child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in various forms of media, including media stored on digital media storage devices such as computers, tablets, cellphones, etc. I am a graduate of the Criminal Investigator Training Program ("CITP"), and the HSI Special Agent Training ("HSISAT") at the Federal Law Enforcement Training Center in Glynco, Georgia. I have participated in the execution of previous search warrants, which involved child exploitation and/or child pornography offenses, and the search and seizure of computers, related peripherals, and computer media equipment. I am a member of the Seattle Internet Crimes Against Children Task Force ("ICAC"), and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

PURPOSE OF AFFIDAVIT

3. This affidavit is submitted in support of an application for a search warrant for the Facebook accounts associated with Kenneth Merlin Richens ("RICHENS")(as defined in Attachment A), for the items to be seized as described in Attachment B, which are the evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a)

(production of child pornography); 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5) (receipt, distribution, transportation, possession of/access with intent to view child pornography); 2422(b) (coercions/enticement) (the "crimes under investigation"). Attachments A and B are attached hereto and incorporated herein by reference.

4. The statements in this affidavit are based upon my personal observations, my training and experience, my investigation into this case and, information obtained from various law enforcement personnel and witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. All dates set forth below are on or about the dates indicated, and all amounts or sums are approximate.

SUMMARY OF PROBABLE CAUSE

5. As set forth in detail below, Kenneth RICHENS lives in Nephi, Utah. Earlier this year RICHENS traveled to the Philippines. He returned to the United States on or about March 30, 2023. While he was traveling back to Utah, RICHEN's initial re-entry into the United States was at SeaTac International Airport in Seattle, Washington. Customs agents sent RICHENS to secondary inspection and attempted a border search on multiple electronic devices in his possession. The subsequent border search on a cell phone seized from RICHENS resulted in the discovery of multiple images of child pornography (as defined in 18 U.S.C. 2256 and referred to herein as Child Sexual Abuse Material, or "CSAM"). The search also resulted in the discovery of evidence suggesting

that RICHENS has used Facebook messenger to receive child pornography and to communicate with others about paying for child pornography. By this affidavit I seek permission to search the Facebook accounts associated with RICHENS.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Computer technology revolutionized the way individuals interested in child pornography interact with each other. Child pornography previously was produced with traditional cameras and film (i.e. still photography and or movies). Photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce images. Both the production process and or large-scale distribution of images required significant resources. Photographs themselves were bulky and required secure storage in order to prevent public discovery. The distribution process required a combination of personal contacts, mailings and telephone calls.

7. Today's computer technology replaces the antiquated methods of production, communication, distribution, and storage of child pornography. In contrast, child pornographers convert traditional photographs to a digital format using a common scanner. With the advent of digital cameras, images are transferred directly (and in mass quantities) onto a common computer hard drive. A device known as a modem allows any computer to connect to other computers around the globe via phone, cable, wireless, or satellite internet connection. This digital web links millions of computers around the world. Moreover, the technical ability to store vast amounts of digital images to discreet devices (i.e. laptops, tablets, and or smartphones) makes these common and relatively inexpensive devices an ideal repository for child pornography. The size of the electronic

storage media (commonly referred to as the hard drive) used in common home computers, laptops, tablets, smart-TVs or smart-phones has grown exponentially within the last several years. These hard drives can store tens of thousands of digital images at very high resolution.

8. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Facebook, Google, Yahoo!, Dropbox, and Hotmail, among others. Online services permit a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with internet access.

9. Generally, electronic communications via computer may be saved and or stored on the computer used to communicate. Storing this information can be *intentional* by saving an e-mail as a file on the computer or saving the location of one's favorite websites (i.e. "bookmarks"). Digital information may be retained *unintentionally.* Traces of the path of an electronic communication may be automatically stored in several locations (i.e. temporary files or ISP client software). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Additionally, a forensic examiner often can recover evidence suggesting whether a computer contains

peer-to-peer software (P2P) (which is described in more detail in the following paragraphs), when the computer was sharing files, and the files which were uploaded or downloaded. Generally, such information is maintained indefinitely until overwritten by other data.

INTRODUCTION REGARDING PREFERENTIAL SEXUAL OFFENDERS AND THE INTERNET

10. Based upon your affiant's professional experience, training and discussions with other trained law enforcement officers, your affiant learned that there are many types of preferential sex offenders. Some of these offenders have a primary sexual interest in children and often are referred to as pedophiles. This affidavit deals with these types of offenders.

11. Preferential sex offenders receive sexual gratification from actual contact with children and/or from fantasy involving children, through the use of photographs and/or digital images that can be stored on computer hard drives and other types of digital recordable media (floppy diskettes, writable compact discs, writable DVDs, etc.). These types of sex offenders often collect sexually explicit material consisting of photographs, video tapes, books, slides, and digital images, which they use for their own sexual gratification, fantasy and or to show children in an attempt to lower the child's inhibitions.

12. The Internet provides preferential sex offenders with a virtually anonymous venue in which they can meet other people with the same or similar sexual interests. Preferential sex offenders also use the computer to electronically exchange

pictures of children or of adults engaged in sexual activity with children. These images are readily available and easily accessible via the Internet. These images can then be downloaded and stored on the computer or other forms of digital recordable media (CD's, DVDs, USB thumb drives) and then viewed on the computer monitor at any time. Preferential sex offenders will also participate in chat rooms in order to communicate with other like-minded individuals and to meet children. This communication serves to legitimize their conduct and beliefs. Preferential sex offenders who collect child pornography rarely dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, and or damage. These individuals typically maintain their child pornography collections in the privacy and security of their homes, or other secure locations for lengthy periods of time.

FACEBOOK

13. Facebook Inc. (“Facebook ”) is an internet service provider located at1601 Willow Road, Menlo Park, California 94025. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com or through its app. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

14. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user’s full name, birth date, gender, contact e-mail

addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

15. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

16. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

17. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates

about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

18. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

19. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive

instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

20. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

21. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

22. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

23. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

24. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

25. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

26. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

27. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

28. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of

the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the

Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Therefore, the computers of Facebook are likely to contain stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

SEARCH METHODOLOGY TO BE EMPLOYED

30. This warrant is sought pursuant to the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(l)(A). Facebook will be directed to disclose copies of the records and other information (including the content of communications) particularly described in Attachment B. Law enforcement executing the warrant will then search the electronic data contained in the records received from Facebook. A non-exclusive list of the search procedures that may be used to examine this data includes:

a. examination of all of the data contained in the records to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the

offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contained. opening files in order to determine their contents (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files.

d. "opening' or cursorily reading the first few "pages" of such files in order to determine their precise contents.

e. scanning storage areas for deliberately hidden files; or

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

31. Based upon my specialized, professional knowledge, training, and experience, and in consultation with HSI experts in this field, I know that searching and seizing information from large amounts of data may require an agent to need the assistance of a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. **The volume of evidence.** The Facebook file may store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store items in random order with deceptive file names.

This may require searching authorities to examine all the stored data to determine which particular files are evidence of instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. **Technical requirements.** Searching large quantities of data obtained from systems for criminal evidence may become a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

STATEMENT OF PROBABLE CAUSE

32. RICHENS is a resident of Nephi, Utah. He is employed as the Chief Information Officer at Central Valley Medical Center in Utah, which lists RICHENS on the Executive Leadership page of its website. RICHENS' LinkdedIn account also lists him as the "President of Educational Hope for Children." According to its website, Educational Hope for Children is a non-profit organization "dedicated to providing

educational opportunities for disadvantaged youth and children around the world." The website also indicates that it currently has ongoing projects in Philippines and Cambodia, working to serve orphans and economically disadvantaged students. A photo resembling RICHENS is displayed on the website.[1]

33. Law enforcement databases indicate that RICHENS has traveled to the United States from Manila, Philippines, approximately 49 times since 2011. RICHENS also appears to have traveled to the United States from Bangkok, Thailand; Tokyo, Japan; and Seoul, South Korea one to two times. RICHENS also traveled in the past one time from Salt Lake City, Utah to Phnom-Penh, Cambodia.

34. Based on my training and experience, the Philippines, Thailand, and Cambodia are all common destinations for child sex tourism.

35. On or about March 30, 2023, Kenneth RICHENS presented himself for entry into the United States at SeaTac International Airport. He traveled from Manila, Philippines, via Seoul, South Korea, and his final destination was Salt Lake City, Utah. Customs agents sent RICHENS, traveling alone, to secondary inspection. RICHENS had a number of electronic devices in his possession, but all were password protected. RICHENS declined to provide the password(s) for any of the electronic devices, stating that he wanted an attorney to verify that whether there was anything illegal on them. Officers told RICHENS they would detain the devices and examine them. HSI took the

[1] This is based on known images of RICHENS such as the photo on his Utah state driver license.

seized devices to the HSI Seattle computer forensics lab for examination, and RICHENS continued his travel back to Utah.

36. HSI Seattle Computer Forensics Analyst (CFA) Royal was able to access data on two cellular telephones seized from RICHENS. There were files establishing that the devices belonged to RICHENS – for example, there were numerous photographs depicting RICHENS with children at what appears to be a school in the Philippines. There was also a video depicting RICHENs having sex with a girl whose appearance is consistent with Filipino/southeast Asian descent. (She is approximately 19 years old based on a driver's license photograph also found in RICHENS' devices.)

37. In addition, there were a number of files that appear to be child pornography/CSAM found on RICHENS' cellphones. These images generally depict young children of Filipino/southeast Asian descent. The devices on which these images were found have cameras. Is not clear whether these images were taken by RICHENS. If they were not produced by RICHENS, however, he received them from somewhere.

38. Once these images were found the border search of his devices stopped in order for agents in the Seattle area to seek a search warrant.

39. I have reviewed these files and agree that many images appear to be child pornography/CSAM. Some files depict prepubescent children fully nude from head to toe engaged in what may be non-sexual activity, such as showering. However subsequent pictures appear to depict the same children but closeup images depicting only their genitals. In some of the images, the boys have erect penises both in the full body

pictures and in the closeups of their penises. In others the children are being subjected to sex acts with what appear to be adult men.

40. Five examples of the files I reviewed are described below:

a. A file named 8944299072546836940.0 depicts a young boy, approximately 5 years old based on his size, lack of muscular development, lack of pubic hair, and lack of development of the child's genitalia. His appearance is consistent with a child of Filipino/southeast Asian descent. The child is lying on his back on a bed. The bed has blue sheets, a grey blanket, and a red "Hello Kitty" patterned pillowcase. The child is naked but for an orange shirt, which is pulled up to expose his bare stomach and penis. The child is looking down towards his exposed penis.

b. A file named -9166614210836296622.0 depicts a naked child from the chest to upper thigh area, focused on the boy's exposed penis. While the boy's face is not visible, this appears to be the same child described in photograph above, because his body appears the same and he appears to be lying on the same bed with the same gray blanket.

c. A file titled received_1255519071909588.mp4 is a video depicting an adult man with a girl who appears to be approximately 12 years old. The child's age is based on her size relative to the adult male as well as the lack of pubic hair and youthful facial features. The adult man is white. The child's appearance is consistent with a child of

Filipino/southeast Asian descent. In the video, the child is lying on her back with her legs raised. While she is wearing a long-sleeved shirt and pants, her pants are pulled down to bunch around her thighs, exposing her vagina. The white male adult is kneeling below the child on the bed, exposing his erect penis. His hands are on the back of the child's thigh to keep her propped on her back with her legs raised, and he is vaginally penetrating the child with his penis. The adult male's face is not visible but he is wearing a white shirt with red and blue stripes and red long-sleeves.

d. A file titled 45362.jpg depicts a young boy standing facing the camera. He appears to be between 9 and 11 years old based on the child's overall size, stature, lack of muscular development, lack of pubic hair development, and the development of the child's genitalia. The child's appearance is consistent with a child of Filipino/southeast Asian descent. The child has no shirt on and is pulling his pants or underwear down with both hands to expose his penis. The child is visible from the pelvic area and up, to include the child's face.

e. A file titled -290552208177152534.0 depicts a male child, approximately 10 and 12 years old based on his physical stature and lack of body hair. He lying naked on a bed, with his legs spread apart to expose his genital area and anus while an adult male had penetrates his anus with a finger. The photograph depicts the child from chest to mid-

thigh, making the genital area and penetrated anus the focus of the picture.

41. **Identification of RICHENS FACEBOOK ACCOUNT**. Digital artifacts reviewed on RICHENS' cellphones indicate that RICHENS uses a Facebook account with Facebook ID 100024578089227 (the "RICHENS FACEBOOK ACCOUNT"). For example:

a. Digital artifacts on the phones seized from RICHENS indicate that the RICHENS FACEBOOK ACCOUNT was accessed from these devices.

b. The username on the RICHENS FACEBOOK ACCOUNT is "nek snehcir" which appears to be "Ken Richens" spelled backwards.

c. The password for the RICHENS FACEBOOK ACCOUNT is the same as the passwords for RICHENS' devices that were in his possession when he was initially encountered.

d. The user of the RICHENS FACEBOOK ACCOUNT identified himself as Kenneth Richens in a message sent from that account. Specifically, in a Facebook message sent from the RICHENS FACEBOOK ACCOUNT to another user, the message reads, "This is Kenneth Richens. Account number 703290426. I have been unable to login to my account to pay my monthly cable bill for Shell Residences unit 1624 D". Other photos of documents found on RICHENS' devices show the Shell Residences unit 1624 D to be in RICHENS name.

42. Further, evidence establishes probable cause to believe that RICHENS used his Facebook account to communicate with others about his sexual interest in children,

including young boys, and to discuss/arrange payment in exchange for child pornography.

43. Artifacts found in RICHENS' cellphones indicate that on or about March 21, 2023, at approximately 2:21:23 am, the user of the RICHENS FACEBOOK ACCOUNT created a Facebook Messenger chat group. The artifact indicates that he edited the chat description from "general chat" to "Stay connected to sharing cute boys videos in real time with on and off topic chats."

44. Screenshots found on one of RICHENS' cellphones appear to show excerpts from Facebook messenger message threads. Some of the screenshots do not identify the Facebook accounts participating in these message threads. However, some show that the RICHENS FACEBOOK ACCOUNT was one of the participants. For example, in one screen shot, the RICHENS FACEBOOK ACCOUNT was communicating with Facebook messenger username "Emmanuel Reyes Delacruz." In that message thread, RICHENS tells Emmanuel, "You broke my heart when you stopped chatting with me because I would not keep giving you money for video."

45. In a second screen shot depicting a conversation with Emmanuel, Emanuel sent child pornography:

> Emmanuel: Emmanuel unsent a message
> Sender: Unsend?
> Emmanuel: Emmanuel unsent a message
> Emmanuel: [Sends an image of a boy, approximately 12-14 years old. Consistent with the other images of child pornography found on defendant's phone, this boy appears to be of Southeast Asian descent. He is naked. The photograph depicts the boy from his face to upper thigh, reclining naked on a red Mickey Mouse patterned bed spread, exposing his penis. This screen shot image has a "last write time" of May 16, 2022. The

image of the child in this screen shot matches an image file located on one of RICHENS'cellphones. The last write time on that file is 9/6/2022.

46. Two screen shots on RICHENS' cellphone depicted a Facebook messenger conversation with a recipient using an avatar depicting two dark haired females. The "last write time" associated with these screen shots is June 26, 2020.

a. The first screen shot indicated:

Sender: No, she did not want to be with me last time
Recipient: Why she is diba
Recipient: I have here picture
Recipient: I have now 10pictures Janet
Sender: No, we agreed Micaela and Princess before

b. The second screen shot with this same recipient indicated:

Recipient: many pics
Recipient: many positions
Sender: You said that before
Recipient: Princess and micaella
Recipient: So if I send you thats I wish you helping me
Sender: 100 for each good picture
Sender: Nothing for bad

47. A third screen shot depicts an excerpt of a Facebook message thread with a recipient username, "Jhan Mhar." The message exchange captured is as follows:

Sender: Show me your body. Then I will agree.
Jhan Mhar: [Sends an image of a male sitting in a dark room on what appears to be a white toilet seat. The male has both hands clasped together to cover his genital area. Due to the poor lighting and photo quality it is difficult to determine an approximate age on the male.]
Jhan Mhar: Its too dark

48. Another digital forensic artifact from RICHENS FACEBOOK ACCOUNT shows a chat excerpt between the RICHENS FACEBOOK ACCOUNT and Facebook username "Yheshie Sundian." "Yeshie Sundian" asks the RICHENS FACEBOOK

ACCOUNT, "My friend when can I make video again?" The RICHENS FACEBOOK ACCOUNT replies, "I really don't want video. Always the same people."

a. Facebook user "Yheshie Sundian" is associated with Facebook ID 100015152076845 and appears to have had a previous username of "Rdel Sundian".

b. On June 5, 2023, HSI Seattle issued a summons for account data and transaction history related to RICHENS' account with Remitly, Inc. Remitly, Inc. is an American online money transfer service specializing in international money transfers. On June 6, 2023, Remitly, Inc. provided transaction history for RICHENS' Remitly account which included two transactions to a recipient, "Rodel Sundian," located in the Philippines. The two transactions sent to "Rodel Sundian" occurred in July 2021 and totaled approximately $120 USD.

49. **There is Probable Cause to Believe Evidence of Criminal Activity Will be Located in the Facebook accounts associated with Ken Richens, including the RICHENS FACEBOOK ACCOUNT.** As set forth above, there is probable cause to believe that RICHENs travelled to the Philippines and recorded himself having sex with a young woman who appears to be of Filipino descent. He took multiple photographs of himself in the presence of children who appear to be of Filipino descent. He also possessed a number of CSAM files depicting young children who appear to be of Filipino descent, although these images do not depict the face of the person taking the pictures. He also brought these images back with him from the Philippines to the United States.

50. Based on this evidence, there is probable cause to believe that RICHENS is someone with a sexual interest in children and images of children. Based upon my

knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals with a sexual interest in children and images of children; these characteristics contribute to the likelihood that evidence will be found on his person and in his home, and include:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect, possess, or view sexually explicit or suggestive materials in a variety of media. In the past, this media commonly included hard copy materials such as photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. More recently, such individuals may collect, possess or view such sexually explicit materials in digital format, stored on devices in their possession or remotely in cloud storage. For example, RICHENS appears to have stored such material on his cellphones but also used the RICHENS FACEBOOK ACCOUNT to receive child pornography via the cloud.

c. Regardless of how the materials are stored, individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

d. Likewise, such individuals (like RICHENS) who maintain their child pornography images in a digital or electronic format typically do so in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to easily view the child pornography images. For example, RICHENS had child pornography on digital devices secured by a password so they were both secure and able to be carried with him and accessed even when he travelled. He could use these same devices to easily access material stored in the cloud, in locations such as Facebook.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This is evidenced by RICHEN's screen shots of his communications with individuals using Facebook messenger to discuss payments for images and videos.

f. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. For example, RICHENS brought the images with him digital devices as he traveled; the fact

that he risked bringing them through customs indicates how highly he values such images.

51. Furthermore, there is probable cause to believe that RICHENS travelled to and from the Philippines and transported child pornography as part of this travel. Based on my training and experience, messenger applications such as Facebook are commonly used to communicate with individuals overseas and also to post photographs of travels, etc. It is likely that evidence of RICHENS' travel to and within the Philippines and other countries in Eastern Asia will be found in the RICHENS FACEBOOK ACCOUNT.

52. Further, there is probable cause to search for any evidence tending to identify the children depicted in the child pornography images. This would include evidence of RICHENS's travels to the Philippines and other places in southeast Asia, any communications with individuals regarding images and videos of minors and paying for the receipt or production of such images and videos, and possible arrangements to meet these individuals or minors in person while RICHENS was traveling.

CONCLUSION

53. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein (the crimes under investigation") have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the Facebook accounts described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

54. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items sent from Facebook in response to the search warrant. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,

/s/ALAINA DUSSLER

_____

Alaina Dussler
Homeland Security Investigations

Sworn to before me and signed in my presence
and/or by reliable electronic means.

Cecilia M. Romero

_____

Hon.
United States Magistrate Judge

ATTACHMENT A
PROPERTY TO BE SEARCHED

The property to be searched is any Facebook account associated with Kenneth Merlin Richens, including but not limited to Facebook ID 100024578089227 (the "RICHENS FACEBOOK ACCOUNT)", the contents of which are currently in the possession of Facebook Inc. (the "PROVIDER"), located at 1601 Willow Road, Menlo Park, California 94025.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Pursuant to 18 U.S.C. § 2703, the PROVIDER as described in Attachment A is hereby ordered as follows:

I. SEARCH PROCEDURE

a. The search warrant will be presented to personnel of Facebook Inc., who will be directed to isolate those accounts and files described in Section II below;

b. In order to minimize any disruption of computer service to innocent third parties, Facebook Inc. and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;

c. Facebook Inc. will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant; and

d. Law enforcement personnel will thereafter review all information and records received from the Facebook Inc. to determine the information to be seized by law enforcement personnel specified in Section III.

II. FILES AND ACCOUNTS TO BE DISCLOSED BY FACEBOOK INC.

For the account listed in Attachment A for the January 2020 to the date that Facebook Inc. collects the data in response to this order, Facebook Inc. shall disclose the following information, and the disclosure shall include all information even if deleted yet still available to Facebook Inc., all information preserved pursuant to a request under 18 U.S.C. § 2703(f), regardless of whether such information is located within or outside of the United States:

1. The contents of all communications, emails, messages, and attachments associated with the accounts listed in Attachment A, including deleted, stored, or preserved (pursuant to 18 U.S.C. § 2703(f) or otherwise) emails sent to and from the account, draft emails, existing printouts of any such emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

2. All records or other information regarding the identification of the accounts listed in Attachment A, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses, phone numbers, or other identifying information provided during registration, other associated email accounts, all screen and usernames (past and current) associated with the subscribers and/or accounts, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

3. All transactional information of all activity of the account or identifier described above, including log files, messaging logs, dates and times of connecting, methods of connecting, IP addresses associated with the outgoing and incoming messages;

4. All messaging and/or transactional logs, including date and time of messages and identification numbers associated with the device sending and receiving message;

5. All records or other information regarding the devices associated with, or used in connection with, the account (including all device identifier information or cooking information, all current and past trusted or authorized devices and computers, and any devices used to access Provider's services) including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

6. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

7. All records indicating the services available to subscribers of the accounts listed in Attachment A.

8. The services and types of services the accounts listed in Attachment A utilized and all records generated by those services;

9. All records or other information stored at any time by an individual using the accounts listed in Attachment A, including address books, contact and buddy lists, calendar data, pictures, and files;

10. Identity of other accounts or services sharing the recovery account or telephone number or other two-factor authentication methods used for the accounts listed in Attachment A and the services the accounts listed in Attachment A used and all records generated by those services;

11. All information obtained from any cookies, beacons, geotags or pixel tags associated with the accounts listed in Attachment A;

12. All location information associated with the accounts listed in Attachment A;

13. All web history, including search terms for the accounts listed in Attachment A;

14. All records indicating the services available to subscribers of the accounts listed in Attachment A;

15. All records or other information stored at any time by an individual using the accounts listed in Attachment A, including address books, contact and buddy lists, calendar data, pictures, and files;

16. All information about the device or devices used to access or use the accounts listed in Attachment A;

17. All privacy and account settings;

18. All records pertaining to communications between the Facebook Inc. and any person regarding the accounts listed in Attachment A, including contacts with support services and records of actions taken.

19. A list of all of the people that the user follows and all people who are following the user (i.e., the user's "following" list and "followers" list), as well as any friends of the user;

20. A list of all users that the account has "unfollowed" or blocked;

21. All records of searches performed by the account, including all past searches saved by the account;

22. All information about connections between the account and third-party websites and applications;

23. All data and information associated with any profile page, including photographs, "bios," and profile backgrounds and themes;

24. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends

logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

25. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to the Provider (e.g., including, but not limited to, keybag.txt and fileinfolist.txt files).

26. All records and information regarding locations where the account or devices associated with the account, including all data stored in connection with any location based services, maps, or other services used.

III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT PERSONNEL

a. All information described above in Section II that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2251(a), 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5); and 2422(b) (hereinafter the "crimes under investigation:")

1. All electronic mail, attachments, messages, and related computer files or information that identify the account creator, user, individuals, or correspondents engaged in the production, sharing, receipt, collection, or possession of child pornography, or that identifies the means or methods used regarding such or other violations of the crime under investigation;

2. All "address books" or other lists of correspondents relevant to the crime under investigation;

3. All saved "chat" or messaging transcripts that reflect an interest in sexual exploitation of minors and/or otherwise relevant to the crime under investigation;

4. Any and all records, documents, visual depictions, and materials pertaining to child pornography, child erotica, an interest in such materials, or pertaining to a sexual interest in children, or sexual activity involving children;

5. Any and all information, notes, software, documents, records, or correspondence, in any form and medium pertaining to any minor who is, or appears to be, the subject of any visual depiction of child pornography, child erotica, sexual activity with other minors or adults, or of sexual interest, or that may be helpful in identifying any such minors;

6. Images, correspondence, and other records that help identify the user of the accounts listed in the Attachment A;

7. Content of web history and searches that reflect interest in sexual activity with children and the crime under investigation;

8. Content of web history and search that reflect a sexual interest in or the sexual exploitation of minors or that help identify persons possessing, receiving, distributing or producing child pornography or the crime under investigation;

9. Location information associated with the accounts listed in Attachment A that is relevant to the crime under investigation that helps identify the user of the account or events relating to the crime to determine the chronological and geographic context of account access, use, and events relating to the crime and to the accounts listed in Attachment A, owner and the owner's contacts that are evidence of the crime under investigation;

10. Location information associated with the accounts listed in Attachment A that may help identify suspects, the account user, or show where events occurred, and who sent, received, possessed or produced child pornography or other evidence of the crime under investigation;

11. Information obtained by Facebook Inc. using cookies, web beacons, or pixel tags that help identify who may have participated in the crime under investigation;

12. Information about the devices used to access the accounts listed in Attachment A that is evidence of or identifies persons involved in the crime under investigation;

13. Information about the devices used to access the accounts listed in Attachment that is evidence of or identifies persons possessing, receiving, distributing or producing child pornography or other violations of Title 18, United States Code, Sections 2251(a), 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5);

14. EXIF or other metadata about images, documents or correspondence reflecting a sexual interest in children, or that help identify the device or person who produced, sent, traded, received, or possessed child pornography or that identifies the user of the accounts used to engage in child exploitative acts.

15. EXIF or other metadata about images, documents or correspondence reflecting an interest in the sexual exploitation of minors or that help identify the device or person using the account or that otherwise is evidence of the crime under investigation;

16. Information about the devices used to access the accounts listed in Attachment A that is evidence of or identifies the user of the account or persons producing, possessing, receiving, distributing or producing child pornography or other violations of the crime under investigation;

17. Information about the devices used to access the accounts listed in Attachment A that is evidence of or identifies the user of the account or persons involved in the crime under investigation;

18. Records and information concerning communications between individuals about the crime under investigation or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography or that is evidence of the crime under investigation.

19. Records and information concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members, and/or that advertise, promote, discuss or otherwise involve child pornography;

20. Records and information concerning membership in online groups, clubs, or services that discuss or otherwise involving the crimes under investigation;

21. Records and information related to the known associates, or any others associated with the accounts listed in Attachment A, including biographical information, addresses, email addresses, user names, social security numbers, or other pertinent identifying information;

22. Evidence indicating how and when the accounts listed in Attachment A was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

23. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

24. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;

25. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;

26. Records relating to who created, used, or communicated with the accounts listed in Attachment A or identifier, including records about their identities and whereabouts.

IV. ORDER OF NON-DISCLOSURE AND ORDER NOT TO TAKE ADVERSE ACTION AGAINST THE ACCOUNT

a. Pursuant to 18 U.S.C. §§ 2703(b)(1)(A) and 2705(b), the Court orders Facebook Inc. not to disclose the existence of this search warrant to any person for the period of one year, including the subscriber, other than its personnel essential for compliance with the execution of this warrant.

b. So as not to disrupt this ongoing investigation and so as to not to otherwise notify the subscriber, the Court further orders Facebook Inc. that it is not to take adverse action against the accounts listed in Attachment A, such as shutting it down, because of this Warrant.

V. PROVIDER PROCEDURES

c. Facebook Inc. shall deliver the information set forth above within 14 days of the service of this warrant and the Facebook Inc. shall send the information electronically or via United States mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium, to:

Special Agent Alaina Dussler

HSI SAC Seattle

1000 2nd Ave Ste 2300

Seattle, WA 98104

d. Pursuant to 2703(g), the presence of an agent is not required for service or execution of this warrant.

V. DEFINITIONS

a. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored.

b. “Child Pornography” as used herein is defined in 18 U.S.C. § 2256(8). (Any visual depiction, including any photograph, film, video, picture, or computer or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

c. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is _____. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook.; and

c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature